# *Binary Modular Groups and their Invariants.*

By Leonard Eugene Dickson.

1. In the first part of this paper I determine all subgroups of the group $\Gamma$ composed of all binary transformations of determinant unity with coefficients in the Galois field $F$ of order $p^n$. The order of $\Gamma$ is

$$\omega = p^n(p^{2n} - 1).$$

I determined the subgroups of $\Gamma$ in the spring of 1904 and made use of the results in investigating* the subgroups of the general ternary and quaternary linear groups modulo $p$, as well as in my study of finite algebras.†

The subgroups of $\Gamma$ may be derived (as in § 9) from the subgroups of the linear fractional group. We may however proceed independently (§§ 2–7). The latter method naturally brings out more clearly the properties of the homogeneous groups, and moreover furnishes material needed in the construction of the invariants (§§ 10–13). The linear fractional groups may be derived by inspection from the homogeneous groups.

The exceptional character of the case $p = 2$ is more marked in the case of homogeneous groups than in the case of fractional groups. Moreover, the homogeneous and fractional groups are identical if $p = 2$. For these reasons I assume here that $p > 2$.

### *Canonical Forms and Conjugacies of the Transformations of* $\Gamma$.

2. Each transformation of $\Gamma$ is given either of the notations

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}: \qquad \begin{aligned} x' &= \alpha x + \beta y \\ y' &= \gamma x + \delta y \end{aligned} \qquad (\alpha\delta - \beta\gamma = 1). \qquad (1)$$

If this replaces a linear function $l$ by $\rho l$, then $\rho$ is a root of the characteristic equation

$$\Delta(\rho) = \rho^2 - (\alpha + \delta)\rho + 1 = 0. \qquad (2)$$

---

*American Journal of Mathematics, Vol. XXVII (1905), Vol. XXVIII (1906).

† *Göttingen Nachrichten*, 1905, pp. 358–393; see § 4.

If $\Delta(\rho)$ is irreducible in $F$, (1) has the canonical form

$$T_\kappa = \begin{pmatrix} \kappa & 0 \\ 0 & \kappa^{-1} \end{pmatrix}, \quad \kappa^{p^n+1} = 1, \quad \kappa^2 \neq 1. \tag{3}$$

If $\Delta(\rho)$ has two distinct roots in $F$, (1) is conjugate within $\Gamma$ with

$$T_\lambda = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \quad \lambda^{p^n-1} = 1, \quad \lambda^2 \neq 1. \tag{4}$$

But if the roots are equal, (1) is conjugate within $\Gamma$ with

$$S_{\pm 1, \beta} = \begin{pmatrix} \pm 1 & \beta \\ 0 & \pm 1 \end{pmatrix}. \tag{5}$$

Now $T_\lambda$ transforms $S_{\pm 1, \beta}$ into $S_{\pm 1, \lambda^2\beta}$. Thus the transformations (5) with $\beta \neq 0$ are conjugate with $S_{\pm 1, 1}$ or $S_{\pm 1, \nu}$, where $\nu$ is a fixed not-square. The latter types are seen to be not conjugate.

*Commutative and Di-cyclic Subgroups.*

3. If $\lambda$ is a primitive root of $F$, $T_\lambda$ generates a cyclic $C_{s-1}$, where $s = p^n$. Here $s > 3$, in view of the assumption (4) that $\lambda^2 \neq 1$. Then the only transformations (1) commutative with $T_\lambda$ are the $T_\alpha$, and the only ones transforming $T_\lambda$ into its inverse $T^{\lambda^{-1}}$ are the $T_\alpha T$, where $T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Evidently $T_\lambda$ and $T^{\lambda^{-1}}$ are the only transformations of $C_{s-1}$ conjugate with $T_\lambda$. Hence $C_{s-1}$ is invariant only in a di-cyclic $G_{2(s-1)}$.

A di-cyclic $G_{4k}$ is generated by two operators $A$ and $B$, where $A$ is of period $2k$ and $B^2 = A^k$, $B^{-1}AB = A^{-1}$; it is said to have the cyclic base $C_{2k} = \{A\}$. Two operators $BA^i$ and $BA^j$ ($i < 2k$, $j < 2k$) are conjugate within $G_{4k}$ if and only if $i$ and $j$ are both even or both odd. Since the inverse of $BA^i$ is $BA^{i+k}$, the cyclic $C_4$ generated by the $BA^i$ form one or two conjugate sets according as $k$ is odd or even. Let $d$ be any divisor $>1$ of $k$ and set $\delta = k/d$. If $\mu$ is a fixed one of the integers $0, 1, \ldots, \delta - 1$, $BA^\mu$ extends the cyclic base $\{A^\delta\}$ of order $2d$ to a di-cyclic $G_{4d}^{(\mu)}$. These $\delta$ groups are all conjugate within $G_{4k}$ if $\delta$ is odd, or if $\delta$ is even and $k$ odd; but fall into two distinct sets of conjugates if $\delta$ and $k$ are both even. If $d \neq 2$, this process yields every di-cyclic subgroup of $G_{4k}$, since a $G_{4d}$ has a single cyclic $C_{2d}$. If $d = 2$, then $k$ is even and we may set $k > 2$. The only operators of period 4 in $G_{4k}$ are

$$A^{\pm k/2}, \quad BA^i \qquad (i = 0, 1, \ldots, 2k-1).$$

Hence a di-cyclic subgroup $G_8$ contains at least four $BA^i$ and hence two distinct operators $BA^r$ and $BA^s$, not inverse to each other. Thus

$$r \not\equiv s, \quad r \not\equiv s + k \pmod{2k}.$$

Hence $G_8$ contains their product $A^{s-r+k}$, which is neither $A^k$ nor the identity. Hence $G_8$ contains $A^{k/2}$ and may be based on the cyclic $\{A^{k/2}\}$. *Every di-cyclic subgroup of $G_{4k}$ may be based on a cyclic $\{A^\delta\}$, where $\delta = k/d$ is a divisor of $k$. For each divisor $\delta$, there are $\delta$ di-cyclic subgroups $G_{4d} = \{A^\delta, BA^\mu\}$, $\mu = 0, 1, \ldots, \delta - 1$, forming one system or two systems of conjugate subgroups according as $\delta$ and $k$ are not both even or both even.*

In the $GF[p^{2n}]$, $\varkappa^{p^n+1} = 1$ has a primitive root $\varkappa$. Then $T_\kappa$ generates a cyclic $C_{s+1}$, invariant only in a di-cyclic $G_{2(s+1)}$.

We next determine the di-cyclic subgroups of $\Gamma$ whose cyclic bases are subgroups of $C_{s\mp1}$. Now $\Gamma$ contains $\frac{1}{2}s(s \pm 1)$ conjugate cyclic $C_{s\mp1}$, each invariant only in a di-cyclic $G_{2(s\mp1)}$. The latter are all conjugate under $\Gamma$, since an operator which transforms $G$ into $G'$ transforms every operator commutative with $G$ into an operator commutative with $G'$. If $2d_\mp$ is any even divisor $> 2$ of $s \mp 1$ and $\delta_\mp$ is the quotient, $\Gamma$ contains $\frac{1}{2}s(s \pm 1)$ conjugate cyclic $C_{2d_\mp}$, each serving as a cyclic base for $\delta_\mp$ di-cyclic $G_{4d_\mp}$, forming one system or two systems of conjugates under $G_{2(s\mp1)}$ according as not both or both $\delta_\mp$ and $\frac{1}{2}(s \mp 1)$ are even (by above theorem for $k = \frac{1}{2}(s \mp 1)$). For $d_\mp \neq 2$, two subgroups $G_{4d_\mp}$ of $G_{2(s\mp1)}$ are conjugate within the latter if conjugate within $\Gamma$. Indeed, the transforming operator must be commutative with $C_{2d_\mp}$, the only cyclic subgroup of this order in either of the $G_{4d_\mp}$, and hence with the unique cyclic $C_{s\mp1}$ containing it. *Hence if $2d_\mp$ is any even divisor $> 4$ of $s \mp 1$ and the quotient is $\delta_\mp$,* $\Gamma$ *contains in all $s(s^2-1) \div 4d_\mp$ di-cyclic $G_{4d_\mp}$, forming one system or two systems of conjugates according as $\delta_\mp$ and $\frac{1}{2}(s \mp 1)$ are not both even or both even. In the first case a $G_{4d_\mp}$ is invariant only under itself; in the second case, under a di-cyclic* $G_{8d_\mp}$.

Consider next the divisor $2d_\mp = 4$ of $s \mp 1$. The sign $\mp$ must be such that $\frac{1}{4}(s \mp 1)$ is an integer $\sigma$. All the transformations of period 4 of $\Gamma$ belong to the conjugate cyclic $C_{4\sigma}$. Each di-cyclic $G_8$ contains 3 cyclic $C_4$. Now $\Gamma$ contains $\frac{1}{2}s(s \pm 1)$ conjugate $C_4$, each serving as a base for $\delta$ di-cyclic $G_8$. Hence $\Gamma$ *contains in all $\frac{1}{24}s(s^2-1)$ di-cyclic $G_8$.*

A maximum di-cyclic $G_{8\sigma}$ contains $\sigma$ di-cyclic $G_8$, forming one system or two systems according as $\sigma$ is odd or even; namely, according as $s = p^n$ is of the

form $8h \pm 3$ or $8h \pm 1$. Since the $G_{8\sigma}$ are all conjugate under $\Gamma$, it follows that, if $\sigma$ is odd, all the $G_8$ are conjugate; while if $\sigma$ is even, they form at most two systems of conjugates under $\Gamma$. Suppose that, for $\sigma$ even, they form a single system. Then in view of the total number of $G_8$, each would be invariant under exactly 24 transformations of a subgroup $G_{24}$. But, for $\sigma$ even, each $G_8$ is one of $\sigma/2$ conjugates under a certain $G_{8\sigma}$ and is therefore invariant under a subgroup of order 16 of $G_{8\sigma}$. *Hence the* $\frac{1}{24}s(s^2-1)$ *di-cyclic* $G_8$ *contained in* $\Gamma$ *form one system or two systems of conjugates according as* $s = p^n$ *has the form* $8h \pm 3$ *or* $8h \pm 1$. *In the former case, a* $G_8$ *is invariant in exactly a* $G_{24}$*; in the latter case, under a* $G_{48}$.

For $\beta \neq 0$, $S_{1,\beta}$ is of period $p$ and $S_{-1,\beta}$ of period $2p$. Now

$$S_{a,b} = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}, \tag{6}$$

whose inverse is $S_{a^{-1},-b}$, transforms $S_{\pm 1,\beta}$ into $S_{\pm 1,\tau}$, where $\tau = a^2\beta$, while no transformation other than the $S_{a,b}$ transforms $S_{\pm 1,\beta}$ into one of like type. The $2s$ transformations $S_{\pm 1,\beta}$, where $\beta$ ranges over the field, form a commutative group, since

$$S_{\pm 1,\beta} S_{\pm 1,\delta} = S_{1,\pm\beta\pm\delta}, \quad S_{-1,\beta} S_{1,\delta} = S_{1,\delta} S_{-1,\beta} = S_{-1,\beta-\delta}. \tag{7}$$

This commutative group $G_{2s}$ is therefore invariant only under the group $G_{s(s-1)}$ of the transformations (6), and hence is one of $s+1$ conjugates under $\Gamma$. The same is true of the commutative group $G_s$ formed by the $S_{1,\beta}$.

By *Linear Groups*, § 249, with (2; 1) replaced by 1, this $G_s$ has exactly

$$\frac{(p^n-1)(p^n-p)(p^n-p^2)\dots(p^n-p^{m-1})}{(p^m-1)(p^m-p)(p^m-p^2)\dots(p^m-p^{m-1})} \tag{8}$$

subgroups $G_{p^m}$ and each is invariant in a largest group $H$ of order $lp^n(p^k-1)$, where $l = 2$ or 1 according as $n/k$ is even or odd, while the value of $k$ depends upon the particular $G_{p^m}$ chosen. Thus the $G_{p^m}$ is one of a system of $(p^{2n}-1) \div l(p^k-1)$ conjugates under $\Gamma$.

Consider next a subgroup of $G_{2s}$ containing $S_{-1,\beta}$. If $\beta \neq 0$, it contains $S^2_{-1,\beta} = S_{1,-2\beta}$, by (7), and hence $S_{1,c\beta}$, where $c$ is any integer. Hence it contains $S_{-1,\beta} S_{1,\beta} = S_{-1,0}$. Thus in every case the subgroup contains $S_{-1,0} = T_{-1}$, and is therefore a $G_{2p^m}$ given by the extension of one of the preceding $G_{p^m}$ by $T_{-1}$. This $G_{2p^m}$ contains a single $G_{p^m}$, while $T_{-1}$ is invariant under $\Gamma$. Hence, if $m > 0$, $G_{2p^m}$ is invariant only under the above group $H$.

*Non-commutative Subgroups of* $G_{s(s-1)}$.

4. This group $G$ is composed of the transformations (6); viz., $S_{1,\mu}T_a$, where $\mu = b/a$. A rectangular array for $G$ may be formed by taking as the first row the transformations $S_{1,\mu}$, which form the invariant subgroup $G_s$, and as right-hand multipliers the $T_a$ of the cyclic $C_{s-1}$. In any subgroup $G'$ of $G$ the totality* of transformations of period $p$ give rise to a commutative $G_{p^m}$ invariant in $G'$. A rectangular array for $G'$ with the transformations of $G_{p^m}$ in the first row has the property that the transformations in each row are all found in a row of the array for $G$. In fact, two transformations $A$ and $B$ of $G'$ lie in the same row or in different rows of the array for $G'$ according as $AB^{-1}$ is or is not in $G_{p^m}$; namely, is or is not in the first row of the array for $G$. Hence the quotient-group $G'/G_{p^m}$ is a subgroup $G_d$ of the cyclic group $G/G_{p^n}$.

For a $a^2 \neq 1$, the period of $S_{a,b}$ is the exponent to which $a$ belongs, since

$$S_{a,b}^k = S_{a^k,bc}, \quad c = a^{k-1} + a^{k-3} + \ldots + a^{-k+1} = a^{-k+1}\left(\frac{a^{2k}-1}{a^2-1}\right).$$

Hence $G$ contains $2(s-1)$ transformations $S_{\mp 1,\beta}$ of period $p$ or $2p$, and $s^2-3s+2$ of period dividing $s-1$. Hence $G$ contains $s$ cyclic $C_{s-1}^{(b)}$, no two having in common an operator other than $T_{\pm 1}$. They are conjugate within $G$, since $S_{1,\mu}$ transforms $S_{a,b}$ into $S_{a,B}$, where $B = b + \mu(a^{-1} - a)$. Their subgroups $G_d^{(b)}$, for the various divisors $d$ of $s-1$, furnish all the cyclic subgroups of $G$ other than those of period $p$ or $2p$. We proceed as in *Linear Groups*,† p. 271, beginning with line 22, and replacing $G_{p^m}$ by $G_{2p^m}$ (composed of the $S_{\pm 1,\beta}$) in the last line. We conclude that $G'$ *is one of* $p^{n-m}(p^{2n}-1) \div l(p^k-1)$ *conjugates under* $\Gamma$. Here $k$ and $l$ have the same meaning as in § 3.

*Remaining Subgroups Containing Operators of Period* $p$.

5. We proceed as in *Linear Groups*, pp. 272–278, with the following changes.‡ In place of lines 7 and 8 on p. 273, read: "there are $d$ marks $\eta$, the distinct powers of a primitive root of $\eta_0^d = +1$." In equations (251) and (253), replace $\pm 2$ by $+2$. At the bottom of p. 273 and on p. 274, replace (2; 1) by 1.

---

* If no operator of period $p$ occurs, $G'$ is a cyclic subgroup of one of the $C_{s-1}$ and has been listed in § 3.

† In lines 3 and 11 from bottom, change $\infty$, 0 to $\infty$, $\lambda$, and "within which $G_{p^m}$ is self-conjugate" to "which transforms $G_{p^m}$ into itself."

‡ Errata on p. 274: l. 8, interchange $k$ and $m$; l. 14, delete "with $n/k$ odd."

Thus (252) now reads

$$p^m - 1 \leqq d \leqq l(p^k - 1) \leqq l(p^m - 1),$$

whence $k = m$. But $d$ divides $l(p^k - 1)$. Hence either (A) $d = p^k - 1$ or (B) $l = 2$ and $d = 2(p^k - 1)$. On p. 275, line 6, we employ $\varkappa = -1$ (instead of $+1$) and reach the desired result. For $p^k = 3$, the treatment requires the following modification. Since the subgroup contains $P_\eta$, $\eta$ any mark $\neq 0$ in the $GF[p^k]$, it contains the $p^m d = 6$ transformations $V_{1,\lambda} P_{\pm 1}$, $\lambda = 0, 1, -1$. The $\alpha + \delta$ of $V_j' = V_{1,\pm 1} V_j$ is $\alpha_j + \delta_j \pm \gamma_j$, which may be made zero by choice of $\gamma_j = \pm 1$. Employing $P_{\gamma_j} V_j'$, we have the new $\gamma_j$ unity and $\alpha + \delta$ still zero. It follows that, for $p > 2$, the group in case (A) is the total group $B_k$ of transformations of determinant 1 in the $GF[p^k]$.

For use in (B), where $p > 2$, we replace in the lemma on p. 274 period 2 by period 4, namely, $V_j^2 = P^{-1}$. In § 253, there are now $d$ marks $\eta$; the orders of the groups are now twice as great; the dihedron is now di-cyclic. Instead of $T$, we consider the $C_4$ generated by $T_0$. In the third line of p. 277, read "$2fp^k(p^k - 1)$ substitutions of period 4"; in l. 11 read: "distinct from $V_j$ and $V_j P^{-1}$, and of period 4." We thus reach $2(p^k - 1)$ substitutions $V_{\eta,\lambda} V_j$ of period 4, and hence $p^k - 1$ cyclic $C_4$. If $M$ is the number of the $V_j$ leading to a single $C_4 = (V_{\eta,\lambda} V_j)$, the total number of the latter is given in the text. It follows that either $\Omega = 2p^k(p^{2k} - 1)$ or else $\Omega = 120$ and $p^k = 3$. In the first case we employ the subgroup of the $p^k(p^k - 1)$ transformations $V_{\kappa,\lambda}$ (of index 2 under the group of all the $V_{\eta,\lambda}$) and show that it is extended by the $V_j'$ to the group $B_k$ of all binary transformations of determinant 1 in the $GF[p^k]$. Hence $G_\Omega = \{B_k, P_{\eta_0}^2\}$, where $P_{\eta_0}^2$ belongs to $B_k$, and $\eta_0$ is the square root of a primitive root of the $GF[p^k]$. Thus $G_\Omega$ is a group in the $GF[p^{2k}]$.

In the second case, $G_{120}$ has one set of $1 + fp^k = 10$ conjugate $C_3$, and one set of 15 conjugate $C_4$ each invariant in exactly a di-cyclic $G_8$. Hence there are 5 conjugate $G_8$. It is shown in §§ 6, 7 that $G$ is of the homogeneous icosahedral type and occurs as a subgroup of $\Gamma$ in the $GF[3^n]$, $n$ even.

As in § 255, the largest subgroup of $\Gamma$ in which the total binary $B_k$ in the $GF[p^k]$ is invariant is $B_k$ if $n/k$ is odd, and $\{B_k, P_{\eta_0}\}$ if $n/k$ is even; while the latter is invariant only under itself. The groups of the latter type (occurring only when $n/k$ is even) form 2 systems of conjugates under $\Gamma$. The groups of type $B_k$ form two systems of conjugates if $n/k$ is even, and one system if $n/k$ is odd.

*Subgroups Containing no Operator of Period p.*

6. Every transformation other than $T_{\pm 1}$ of such a subgroup $G_\Omega$ lies in a unique largest cyclic subgroup $C_d$ of $G_\Omega$. Two such $C_d$ have in common no operator other than $T_{\pm 1}$. According as $C_d$ is invariant within $G_\Omega$ only under itself or under a di-cyclic* $G_{2d}$ based on $C_d$, it is one of a system of $\Omega/d$ or $\Omega/2d$ conjugates under $G_\Omega$. Let $r$ be the number of such systems. The enumeration of the transformations of $G_\Omega$ leads to the relations

$$\Omega = \delta + \sum_{i=1}^{r} (d_i - \delta) \frac{\Omega}{t_i d_i} \qquad (f_i = 1 \text{ or } 2), \qquad (9)$$

$$\Omega \geqq f_i d_i \qquad (i = 1, \ldots, r), \qquad (10)$$

where $\delta = 2$ if $G$ contains $T_{-1}$, $\delta = 1$ if it does not. Indeed, if $G$ contains $T_{-1}$, every $G_{d_i}$ contains $T_{-1}$. Since $T_{-1}$ is the only transformation of period 2, it suffices to show that $d_i$ is even. If $S$ is of odd period $\sigma$, $S T_{-1}$ is of period $2\sigma$ and $(S T_{-1})^{\sigma-1} = S^{-1}$, so that the cyclic $\{S T_{-1}\}$ contains $S$. Next, if $G$ does not contain $T_{-1}$, $\Omega$ and each $d_i$ are odd. In each case $\Omega$ and $d_i$ are multiples of $\delta$ and we may set

$$\Omega = \Omega' \delta, \quad d_i = d_i' \delta, \qquad (i = 1, \ldots, r).$$

When these values are inserted in (9) and (10), we obtain the relations, written in accented letters, at the beginning of § 256 of *Linear Groups.* Employing the results obtained, we reach the following conclusions. If $r = 1$, then $f_1 = 1$, $\Omega' = d_1'$, and $G$ is a cyclic $C_{d_1}$. If $r = 2$, we may interchange $f_1$ and $f_2$ if necessary and set $f_1 = 1$, $f_2 = 2$. Either $d_1' = 2$, $\Omega' = 2d_2'$, or $d_1' = 3$, $d_2' = 2$, $\Omega' = 12$. In each case, $\Omega$ is even and $G$ contains $T_{-1}$, so that $\delta = 2$. In the first case, $d_1 = 4$, $d_2 = 2d_2'$, where $d_2'$ is odd (otherwise $C_{d_1}$ would not be maximal), and $G$ is a di-cyclic $G_{2d_2}$, already considered (§ 3). In the second case, $d_1 = 6$, $d_2 = 4$, $\Omega = 24$. Thus $G_{24}$ contains a system of 4 cyclic $C_6$ each invariant only under itself. Since they have only $T_{\pm 1}$ in common, $G_{24}$ is isomorphic with a subgroup $G_{12}^{(4)}$, necessarily the alternating group on 4 letters. Since the latter has an invariant $G_4$, $G_{24}$ has an invariant $G_8$. This also follows from the fact that the 4 $C_4$ contain 8 operators of period 6, 8 of period 3, so that there are at most 8 operators of periods powers of 2; but $G$ contains a di-cyclic $G_8$ based

*Dihedron in the case $p = 2$ not considered here; then $\delta = 1$ below.

on $C_{d_2}$. Hence the di-cyclic $G_8$ is invariant. Thus* $G_{24}$ is of the homogeneous tetrahedral† type, with the generational relations

$$A^4=I,\ B^2=A^2,\ B^{-1}AB=A^{-1},\ C^3=I,\ C^{-1}AC=B,\ C^{-1}BC=AB. \quad (11)$$

Although falling under another heading, we note that, for $p^n=3$, the total group $\Gamma$ is of this type‡ (cf. § 3).

For $r=3$, each $f_i=2$ and we may set $d_3'=2$, whence $\delta=2$. Either $d_2'=2$, $\Omega'=2d_1'$, whence $G_\Omega$ is a di-cyclic $G_{2d_1}$, or $d_2'=3$, $d_1'=3, 4, 5$, $\Omega'=12, 24, 60$, respectively. For $d_1'=3$, we have $d_1=d_2=6$, $d_3=4$, $\Omega=24$; this case is to be excluded, since $C_{d_1}$ is invariant only under a $G_{f_1d_1}=G_{12}$ and hence is one of two conjugates, whereas the operators of $C_{d_2}$ transform it into at least 3 distinct groups. For $d_1'=4$, we have $d_1=8$, $d_2=6$, $d_3=4$, $\Omega=48$. Since $f_i=2$, there are 4 conjugate $C_6$, each invariant in a di-cyclic $G_{12}$. No two of the latter have a $C_3$ in common. Hence the group common to all four $G_{12}$ is a $C_4$ or is composed of $T_{\pm 1}$. The first case is excluded since a $C_4$ is not invariant in $G_{48}$. Hence $T_{\pm 1}$ alone transform each of the 4 conjugate $C_6$ into itself. Thus $G_{48}$ is isomorphic with the symmetric group on 4 letters, having an invariant $G_4$. Hence $G_{48}$ contains an invariant di-cyclic $G_8$. Hence (§ 3) this $G_{48}$ occurs only when $p^n=8h\pm 1$ and is then uniquely determined by its invariant $G_8$. We may determine $G_{48}$ abstractly by the properties that it contains a single operator $A$ of period 2 and that the quotient-group $G_{48}/\{I, A\}$ is of the octahedral type. The latter is generated by $B$ and $C$, where $B^4=C^3=I$, $(BC)^2=I$. Arrange the operators of $G_{48}$ into 24 sets $S_i$, $S_iA$. It must be possible to choose two sets $S_1$, $S_1A$ and $S_2$, $S_2A$ such that

$$S_1^4,\ (S_1A)^4,\quad S_2^3,\ (S_2A)^3,\quad (S_1A^i\,.\,S_2A^j)^2$$

are all in the set $I, IA$. If $S_2^3=I$, then $(S_2A)^3=A$; if $S_2^3=A$, then $(S_2A)^3=I$. Hence, by choice of the notation, we may set $S_2^3=I$. Since $S_1S_2\neq A, I$, we have $(S_1S_2)^2\neq I$. Hence $(S_1S_2)^2=A$. If $S_1^4=I$, then $S_1^2=A$ or $I$, whereas $B^2\neq I$. Hence

$$S_1^4=A,\ S_2^3=I,\ (S_1S_2)^2=A,\ A^2=I,\ AS_1=S_1A,\ AS_2=S_2A. \quad (12)$$

---

* It is not the direct product of $G_8$ and a $C_3$, and hence by Burnside, *Theory of Groups*, p. 103, case (iv), is of type (11). Note that Burnside's proof is faulty; $C^{-3}AC^3$ is $A$ and not $A^{-1}$. But if $C^{-1}BC=B^{-1}A^{-1}$, set $A_1=AB$, $B_1=A^{-1}$. Then $C^{-1}A_1C=B_1$, $C^{-1}B_1C=B^{-1}=ABA^{-1}=A_1B_1$, so that his conclusion is proved.

† $A=(iz_1, -iz_2)$, $B=(-z_2, z_1)$, $C=\left(\frac{(i-1)}{2}(z_1+z_2), \frac{(i+1)}{2}(z_1-z_2)\right)$.

‡ $A=\begin{pmatrix}0&1\\2&0\end{pmatrix}$, $B=\begin{pmatrix}1&1\\1&2\end{pmatrix}$, $C=\begin{pmatrix}1&0\\2&1\end{pmatrix}$, modulo 3.

This is a complete set of generational relations for a $G_{48}$. Indeed, every element can be written in the form $SA$ or $S$, where $S$ is a product of $S_1$, $S_2$, and includes 24 distinct operators in view of the relations defining the octahedral $G_{24}$. This* $G_{48}$ contains a single $G_{24}$ of type (11), 12 operators of period 8, 8 of period 6, 18 of period 4, 8 of period 3, 1 of period 2, and identity. A linear group of this type is given in § 11.

For $d_1' = 5$, we have $d_1 = 10$, $d_2 = 6$, $d_3 = 4$, $\Omega = 120$. Each $C_4$ is invariant only in a di-cyclic $G_8$. Hence there are 15/3 conjugate $G_8$. Thus each $G_8$ is invariant only in a $G_{24}$, necessarily of type (11). The 5 conjugate $G_{24}$ have only $T_{\pm 1}$ in common. Indeed, their common operators form an invariant subgroup of $G_{120}$ and hence of each $G_{24}$. But a homogeneous tetrahedral $G_{24}$ has besides $I$, $C_2$, $G_{24}$ (cases requiring no further discussion) the single further invariant subgroup $G_8$. But the five $G_8$ in the five $G_{24}$ are all distinct. Hence $G_{120}/\{T_{\pm 1}\}$ is the alternating group on 5 letters, viz., an icosahedral group. Further, $G_{120}$ has a single operator $T_{-1}$ of period 2. Hence† there is only one type of such a group and its generational relations are

$$A^2 = I, \quad AB = BA, \quad AC = CA, \quad B^3 = I, \quad C^5 = I, \quad (BC)^2 = A. \qquad (13)$$

Although listed elsewhere, the total group $\Gamma$ for $p^n = 5$ is of this type.‡

*Number and Conjugacy of the Homogeneous Icosahedral Subgroups.*

7. For $p^n = 5$, $\Gamma$ itself is such a $G_{120}$. For $p^n = 5^n$, we employ the result at the end of § 5 and conclude that the $G_{120}$ fall into two systems each of $5^n(5^{2n}-1)/240$ conjugate groups if $n$ is even, but into one system of $5^n(5^{2n}-1)/120$ conjugates if $n$ is odd.

For use below we show that a $G_{120}$ has 120 sets of generators $A$, $B$, $C$. For $p^n = 5$, $\Gamma = G_{120}$ has 6 cyclic $C_5$, and each operator of period 5 is conjugate with at least one $\begin{pmatrix}1 & \mu\\ 0 & 1\end{pmatrix}$, $\mu$ not a multiple of 5. Taking the latter to be $C$, and giving $B$ the form (14), we find that $BC$ has $\alpha' = \alpha + \mu\gamma$, $\delta' = \delta$. Hence $(BC)^2 = A = T_{-1}$ if, and only if, $\alpha + \mu\gamma + \delta = 0$. Thus $\gamma = \mu^{-1}$. Then $\beta = -\mu(1 + \alpha + \alpha^2)$. Thus there are 5 operators $B$ for each $C$ and hence 24.5 sets of generators.

* It is of type 52 in Miller's list, *Quarterly Journal*, Vol. XXX, p. 258.

† Burnside, *Theory of Groups*, p. 377.

‡ For example, $A = \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$, $B = \begin{pmatrix}0 & -1\\ 1 & -1\end{pmatrix}$, $C = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$, modulo 5.

Next, let $p \neq 2$, $p \neq 5$. Then $p^n(p^{2n}-1)$ is divisible by 120 if, and only if, $p^{2n}-1$ is divisible by 5. First, let $\lambda = \frac{1}{5}(p^n - 1)$ be an integer. Let $\rho$ be a primitive root of the field; then $\rho^\lambda$ is of period 5. Set

$$C = \begin{pmatrix} \rho^\lambda & 0 \\ 0 & \rho^{-\lambda} \end{pmatrix}, \quad B = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \quad \alpha\delta - \beta\gamma = 1, \quad \alpha + \delta + 1 = 0.^* \tag{14}$$

Then $BC$ has $\alpha' = \rho^\lambda \alpha$, $\delta' = \rho^{-\lambda}\delta$. Hence $(BC)^2 = A = T_{-1}$ if, and only if,

$$\rho^\lambda \alpha + \rho^{-\lambda}\delta = 0.$$

The three conditions give

$$\alpha = \frac{1}{\rho^{2\lambda} - 1}, \quad \delta = -\rho^{2\lambda}\alpha, \quad \beta\gamma = \frac{-c}{(\rho^{2\lambda} - 1)^2}, \quad c \equiv \rho^{4\lambda} - \rho^{2\lambda} + 1.$$

If $c = 0$, then $\rho^{6\lambda} = -1$, whereas $\rho^\lambda$ is of period 5. Hence to each of the $p^n - 1$ values $\neq 0$ of $\beta$ there corresponds a single value of $\gamma$. But $\Gamma$ contains (§ 3) exactly $\frac{1}{2}p^n(p^n + 1)$ conjugate cyclic $C_5$. Hence there are $2p^n(p^{2n} - 1)$ sets of generators $A$, $B$, $C$ of homogeneous icosahedral subgroups.

Next, let $g = \frac{1}{5}(p^n + 1)$ be an integer. Our group $\Gamma$ is simply isomorphic with the group of binary hyperorthogonal transformations in the $GF[p^{2n}]$:

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}, \quad \alpha\bar{\alpha} + \beta\bar{\beta} = 1, \tag{15}$$

where $\bar{\alpha}$ denotes $\alpha^{p^n}$. Let $B$ have the form (15), so that $\alpha + \bar{\alpha} + 1 = 0$. Set

$$C = \begin{pmatrix} J^g & 0 \\ 0 & \bar{J}^g \end{pmatrix}, \quad J\bar{J} = 1.$$

Now $BC$ is of the form (15) with $\alpha' = \alpha J^g$. Hence $(BC)^2 = T_{-1}$ gives

$$\alpha J^g + \bar{\alpha}\bar{J}^g = 0.$$

For a given $J$, these conditions are satisfied if, and only if,

$$\alpha = \frac{\bar{J}^g}{J^g - \bar{J}^g}, \quad \beta\bar{\beta} = 1 + (J^g - \bar{J}^g)^{-2}.$$

The final sum is an element $\neq 0$ of the $GF[p^n]$, so that there are $p^n + 1$ values of $\beta$. Now $\Gamma$ contains $\frac{1}{2}p^n(p^n - 1)$ conjugate $C_5$. Hence again there are $2p^n(p^{2n} - 1)$ sets of generators of homogeneous icosahedral subgroups.

But each $G_{120}$ has 120 sets of generators. Hence, *when $p^n \pm 1$ is divisible by 5, $\Gamma$ contains in all $p^n(p^{2n} - 1)/60$ homogeneous icosahedral groups.*

---

* This is the necessary and sufficient condition that $B^3 = I$.

In the first case $T_{\rho^e}$ transforms $C$ into itself and $B$ into a transformation with $\alpha$ and $\delta$ unaltered, but with $\beta$ replaced by $\rho^{2e}\beta$. The latter may be made equal to unity or a particular not-square. Since the $C_5$ are all conjugate, it follows that there are at most two systems of conjugate $G_{120}$. But if there were a single system, their number would be at most $p^n(p^{2n}-1)/120$, contrary to the above. Hence* *there are two systems of conjugate homogeneous icosahedral groups within* $\Gamma$, *and each is invariant only under itself.*

In the second case we employ the transformer $T_{J^e}$ to (15) and find that $\alpha$ is unaltered, while $\beta$ is multiplied by $J^{2e}$. But the ratio of two values of $\beta$ is a power of $J$. Hence we may set $\beta = 1$ or $J$. Hence the preceding result holds also in this case.

*Summary of the Subgroups of* $\Gamma$ $(p > 2)$.

8. One invariant $C_2$; $\frac{1}{2}p^n(p^n \pm 1)$ conjugate cyclic $C_{d_\mp}$ for every divisor $d_\mp > 2$ of $p^n \mp 1$; $p^n(p^{2n}-1) \div 4e_\mp$ di-cyclic $G_{4e_\mp}$, forming one system or two systems of conjugates according as $(p^n \mp 1)/2e_\mp$ and $(p^n \mp 1)/2$ are not both even or both even, where $e_\mp$ is any divisor $>2$ of $(p^n \mp 1)/2$; $p^n(p^{2n}-1)/24$ di-cyclic $G_8$, forming one system or two systems of conjugates according as $p^n = 8h \pm 3$ or $p^n = 8h \pm 1$; $N(p^n+1)$ commutative $G_{p^m}$ each one of $(p^{2n}-1) \div l(p^k-1)$ conjugates, where $N$ is given by (8) and $l = 2$ or 1 according as $n/k$ is even or odd, while $k$ depends upon the particular $G_{p^m}$ $(k = n$ if $m = n)$; $N(p^n+1)$ commutative $G_{2p^m}$ each one of $(p^{2n}-1) \div l(p^k-1)$ conjugates; certain systems of $p^{n-m}(p^{2n}-1) \div l(p^k-1)$ conjugate $G_{p^m d_-}$; $l$ systems each of $p^{n-k}(p^{2n}-1) \div l(p^{2k}-1)$ conjugates, of the type of the total binary $B_k$ of determinant 1 in the $GF[p^k]$, $k$ a divisor of $n$; for $n/k$ even, two systems of groups, each invariant only under itself, of the type $\{B_k, T_\epsilon\}$, $\epsilon$ a square root of a primitive root of the $GF[p^k]$; for $p^n = 8h \pm 1$, two systems each of $p^n(p^{2n}-1)/48$ conjugate homogeneous tetrahedral $G_{24}$ and two systems each of this number of conjugate homogeneous octahedral $G_{48}$; for $p^n = 8h \pm 3$, one system of $p^n(p^{2n}-1)/24$ conjugate $G_{24}$; for $p^n = 10h \pm 1$, two systems each of $p^n(p^{2n}-1)/120$ conjugate homogeneous icosahedral $G_{120}$; for $p = 5$, $n$ even, two systems each of $5^n(5^{2n}-1)/240$ conjugate $G_{120}$; for $p = 5$, $n$ odd, one system of $5^n(5^{2n}-1)/120$ conjugate $G_{120}$.

---

*Employing *Linear Groups*, p. 284, and foot-note to p. 285, we may show that the groups fall into a single system within $\{\Gamma, T_\epsilon\}$, where $\epsilon = \rho^{\frac{1}{2}}$, We may show that if $p^n = 5\lambda + 1 = 4t - 1$, there is a single system within the group of binary transformations of determinants $\pm 1$ in the initial field.

For $p=3$ or 5, $G_{24}$ or $G_{120}$ is also listed under $B_k$, $k=1$.

For example, if $p^n=3$, $\Gamma=G_{24}$ contains only the following subgroups other than identity and itself: an invariant $C_2$, an invariant di-cyclic $G_8$, one set of 3 conjugate $C_4$, one set of 4 conjugate $C_3$, and one set of 4 conjugate $C_6$.

*Derivation of the Homogeneous from the Fractional Groups.*

9. The subgroups $G$ of $\Gamma$ may be derived from a list of all linear fractional groups of determinant unity.* If $G$ is of even order $2g$, it contains $T_{-1}$ and hence may be derived from a fractional group $G'$ of order $g$ by replacing each fractional transformation $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ of $G'$ by the two homogeneous transformations $\begin{pmatrix} \pm a & \pm b \\ \pm c & \pm d \end{pmatrix}$. Next, let $G$ be of odd order. Then $G'$ is of order odd and must (by the list cited) be of one of the following types:

(i) A cyclic group of order $d_{\mp}$, an odd divisor of $\frac{1}{2}(p^n \mp 1)$, generated by $\begin{pmatrix} \delta & 0 \\ 0 & \delta^{-1} \end{pmatrix}$, $\delta$ a primitive root of $\delta^d=1$. If the isomorphic homogeneous $H_{d_{\mp}}$ contained $\begin{pmatrix} -\delta & 0 \\ 0 & -\delta^{-1} \end{pmatrix}$, it would be of order $2d_{\mp}$. Hence $H$ is cyclic and generated by $\begin{pmatrix} \delta & 0 \\ 0 & \delta^{-1} \end{pmatrix}$.

(ii) A commutative group of order $p^m$ composed of certain $\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$. The homogeneous $H_{p^m}$ can not contain $\begin{pmatrix} -1 & -\mu \\ 0 & -1 \end{pmatrix}$ of period $2p$. Hence $H$ is composed of the $\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$ with the same range of values for $\mu$.

(iii) A group $G_{p^m d_-}$ given by extending an invariant $G_{p^m}$ by a cyclic $C_{d_-}$. In view of the preceding cases, $H$ is given by the extension of $H_{p^m}$ by a cyclic $H_{d_-}$.

From the list cited we now readily obtain the list in § 8. Note that the former list includes a cyclic group of order any divisor $d_{\mp}$ of $\frac{1}{2}(p^n \mp 1)$. If $d$ is

* *Linear Groups*, p. 285. In the long expression for the number of sets of the $G_{p^m}$, the first factor $p^n-1$ should be $p^{2n}-1$. The reference to Professor Moore's original paper should be changed to *Decennial Publications of the University of Chicago*, Vol. IX (1904), pp. 141–190.

odd, we obtain by (i) a homogeneous cyclic group of order $d$; while by extension by $T_{-1}$ we obtain a cyclic group of order $2d$, a divisor of $p^n \mp 1$. If $d$ is odd, we obtain only the latter type. Hence we reach the homogeneous cyclic $C_{e_\mp}$, where $e$ may be any divisor of $p^n \mp 1$.

### *Invariants of Binary Groups.*

10. Let $G$ be a group, of order $g$, of binary transformations of determinant unity in the $GF[p^n]$. Let $\gamma = 1$ or 2 according as $T_{-1}$ is not or is contained in $G$, and set $\omega = g/\gamma$. A point $(x, y)$, in the sense of homogeneous coordinates, is one of at most $\omega$ distinct conjugates under $G$. A point is called special if it has fewer than $\omega$ conjugates; namely, if it is invariant under some transformations other than $T_{\pm 1}$ of $G$. Each system of special points determines a relative invariant. If we have determined two independent invariants $J$ and $K$ of degree $\omega$ which take on the same factor $f_t$ under each transformation $t$ of $G$, then any invariant $I$ which vanishes for no special point is a product of linear functions of $J$ and $K$. An integral invariant $I$ with coefficients in the $GF[p^n]$ is an integral function of $J$ and $K$ with coefficients in that field.*

### *Invariants of the Cyclic and Di-Cyclic Groups.*

11. Consider a cyclic group of order $d$, a divisor $> 2$ of $p^n - 1$. It is conjugate within $\Gamma$ with a $C_d$ generated by $T_\delta$, where $\delta$ is a primitive root of $\delta^d = 1$. The only special points are $(1, 0)$ and $(0, 1)$, the corresponding invariants being $x$ and $y$. Now $\omega = d$ or $d/2$ according as $d$ is odd or even. Further, $x^\omega$ and $y^\omega$ take on the same factor $\delta^\omega = \delta^{-\omega}$ under $T_\delta$. Hence every invariant is of the form

$$x^i y^j \prod_k (x^\omega + k y^\omega).$$

Next, consider a cyclic group of order $d$, a divisor $> 2$ of† $p^n + 1$. It is conjugate within $\Gamma$ with a $C_d$ generated by

$$S = \begin{pmatrix} l & -1 \\ 1 & 0 \end{pmatrix}, \quad \rho^2 - l\rho + 1 = 0, \text{ irreducible.} \tag{16}$$

Since $S$ has the canonical from $T_\rho$, $\rho$ is a primitive root of $\rho^d = 1$. Now $S$

---

* *Transactions Amer. Math. Society*, Vol. XII (1911), p. 4.

† The present treatment applies also to divisors of $p^n - 1$, but is not as simple as the preceding.

leaves invariant only $(\rho, 1)$, $(\rho^{-1}, 1)$, which are the only special points under $G$. Hence the invariants are functions of

$$\lambda = x - \rho y, \quad \mu = x - \rho^{-1} y. \tag{17}$$

$S$ multiplies these by $\rho^{-1}$ and $\rho$, respectively. The invariants with coefficients in the $GF[p^n]$ can be expressed in terms of the absolute invariant $A = \lambda\mu$ and two linear combinations of $\lambda^\omega$, $\mu^\omega$, for example,

$$B = (\lambda^\omega + \mu^\omega)/2, \quad C = (\lambda^\omega - \mu^\omega)/(\rho^{-1} - \rho). \tag{18}$$

Under $S$ these take on the factor $+1$ or $-1$ according as $d$ is odd or even.

*Examples.* If $p^n = 3$, $d = 4$, then $l = 0$, $A = x^2 + y^2$, $B = x^2 - y^2$, $C = xy$.
If $p^n = 5$, $d = 3$, then $l = -1$, $A = x^2 + xy + y^2$,
$C = 3(x^2 y + xy^2)$, $B = x^3 - y^3 - 3xy^2 + C/2$.

For $2e$ an even divisor of $p^n - 1$, consider the di-cyclic group

$$G_{4e} = \left\{ T_\varepsilon, \ E = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}, \quad \varepsilon^{2e} = 1. \tag{19}$$

The points invariant under a power of $T_\varepsilon$ are $(0, 1)$, and $(1, 0)$, which are interchanged by $E$. The corresponding invariant is $Q = xy$. Next $T_\alpha E$ leaves invariant only $(\pm i\alpha^{-1}, 1)$. Now $-1$ and $\alpha$ are powers of $\varepsilon$. The $e$ points

$$P_k^c = (i\varepsilon^{c+2k}, 1) \qquad (k = 0, 1, \ldots, e-1) \tag{20}$$

form a system of special points. Indeed, $T_\varepsilon$ replaces $P_k^c$ by $P_{k+1}^c$, while $E$ replaces $P_k^c$ by $P_{e-c-k}^c$. For $c = 0$ or $1$, we get the invariants

$$I_c = \prod_{k=0}^{e-1} (x - i\varepsilon^{c+2k} y) = x^e - (i\varepsilon^c)^e y^e. \tag{21}$$

Under $T_\varepsilon$ both $I_0$ and $I_1$ take on the factor $-1$; under $E$, $I_0$ takes on the factor $-(-i)^e$ while $I_1$ takes on the factor $+(-i)^e$. We have the identity

$$I_1^2 - I_0^2 = 4i^e Q^e. \tag{22}$$

If* $p^n = 4l - 1$, so that $i$ does not belong to the field, the fundamental system for invariants with coefficients in the field is $Q$ and $I_0 I_1 = x^{2e} - (-1)^e y^{2e}$.

For $2e$ an even divisor of $p^n + 1$, consider the di-cyclic $G_{4e}$ generated by an operator $B$ of period 4 and an operator $S$ of period $2e$, given by (16), where now $\rho$ is a primitive root of $\rho^{2e} = 1$. Thus $B$ is of the form (1) with $\delta = -\alpha$.

---

* If $p^n = 4l + 1$, we may replace $iy$ by $y$ and obtain the ordinary dihedron invariants.

Then $SB = BS^{-1}$ if and only if $\gamma = \beta + \alpha l$. Introduce the conjugate imaginary variables (17); then

$$S = \begin{pmatrix} \rho^{-1} & 0 \\ 0 & \rho \end{pmatrix}, \quad B = \begin{pmatrix} 0 & -r \\ r^{-1} & 0 \end{pmatrix}, \quad r = \rho(\beta + \rho\alpha), \; -r^{-1} = \rho^{-1}(\beta + \rho^{-1}\alpha). \quad (23)$$

In the new variables $\lambda$, $\mu$, the only points invariant under the powers of $S$ are $(0, 1)$ and $(1, 0)$, which are interchanged by $B$. The corresponding invariant is

$$q = \lambda\mu = x^2 - lxy + y^2. \quad (24)$$

Next, $S^s B$ leaves invariant only $(\pm\, ir\rho^s, 1)$. Now $-1 = \rho^e$. Hence the invariant point belongs to the system

$$P_k^c = (R\rho^{2k}, 1) \qquad (k = 0, 1, \ldots, e-1),$$

where $R = ir\rho^c$, $c = 0$ or $1$. Now $S$ replaces $P_k^c$ by $P_{k-1}^c$, while $B$ replaces $P_k^c$ by $P_{e-c-k}^c$. Thus the corresponding invariants are

$$J_c = \lambda^e - R^e\mu^e. \quad (25)$$

When $\rho$ is replaced by $\rho^{-1}$, $\lambda$ and $\mu$ are interchanged, while $r$ is replaced by $-r^{-1}$, so that $R^e$ is replaced by its reciprocal. Hence*

$$I_c = (1 - R^e)J_c \quad (26)$$

remains unaltered and hence belongs to the field $(F, i)$. In case $i$ belongs to $F$, the fundamental invariants are $q$, $I_0$, $I_1$; in the contrary case, $q$, $I_0 I_1$. Under $S$, $J_c$ takes the factor $-1$; under $B$ the factor $-(i\rho^c)^e$.

For example, let $e = 2$. Taking $l = 0$, we have

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix}, \quad \alpha^2 + \beta^2 = -1. \quad (27)$$

These generate a di-cyclic $G_8$. We may take† $\alpha\beta \neq 0$. Then

$$q = x^2 + y^2, \quad Q_2 = x^2 - 2\alpha\beta^{-1}xy - y^2, \quad Q_3 = x^2 + 2\beta\alpha^{-1}xy - y^2 \quad (28)$$

form a fundamental system for $G_8$. $S$ leaves $q$ unaltered and changes the sign of $Q_2$ and $Q_3$, while $B$ leaves $Q_2$ unaltered and changes the sign of $q$ and $Q_3$. The relation between the absolute invariants is

$$q^2 + \beta^2 Q_2^2 + \alpha^2 Q_3^2 = 0. \quad (29)$$

---

* We note that $R^e$ is not unity for all the $\nu = p^n + 1$ sets of values of $\alpha, \beta$ (each set being given by a root of $r^\nu = -1$); in fact, the $e$ values of $r$ which make $R^e = 1$ are $r = -i\rho^{2k-c}$ $(k = 0, \ldots, e-1)$. In case $e$ and $\nu$ are such that values of $r$ exist for which $R^e = 1$, we may employ the invariants $J_c(\rho - \rho^{-1})$, whose coefficients lie in $F$.

† If the field contains $i$, we may take $\beta = 0$ and obtain a simpler system.

*Invariants of the Total Group and a Related Group.*

12. The group $B_n$ of all binary transformations of determinant unity in the $GF[p^n]$ has (*Transactions, l. c.*) the fundamental system of invariants

$$L = x^{p^n}y - xy^{p^n}, \quad Q = (x^{p^{2n}-1} - y^{p^{2n}-1})/(x^{p^n-1} - y^{p^n-1}). \tag{30}$$

Consider the group $G = \{B_n, T_\epsilon\}$, were $\varepsilon = \rho^{1/2}$, $\rho$ being a primitive root of the $GF[p^n]$. Then $\varepsilon^{p^n-1} = -1$. Hence $T_\epsilon$ multiplies $L$ and $Q$ by $-1$. Thus $L$ and $Q$ form a fundamental system for $G$.

We have noted that, for $p^n = 3$, $B_1$ is of the homogeneous tetrahedral type $G_{24}$. The group $G = \{B_1, T_\epsilon\}$, where $\varepsilon^2 \equiv -1 \pmod 3$ is of the homogeneous octahedral type. Indeed,

$$S_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} T_\epsilon = \begin{pmatrix} \varepsilon & \varepsilon \\ -\varepsilon & \varepsilon \end{pmatrix}, \quad S_2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \quad A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \tag{31}$$

belong to $G$ and satisfy relations (12) which define $G_{48}$. Hence, in treating the invariants of $G_{24}$ and $G_{48}$, we may set $p \neq 3$.

*Invariants of the Homogeneous Tetrahedral and Octahedral Groups.*

13. In view of the preceding remark, we take $p > 3$. If $p^n = 4l + 1$, so that $\sqrt{-1}$ belongs to the field, we may employ Klein's first* form of $G_{24}$; then the fundamental system of invariants with coefficients in the field is† $\phi$, $\psi$, $t$ if $\sqrt{-3}$ belongs to the field, namely, if $p^n = 3k + 1$; but is $\phi\psi$ and $t$ if $p^n = 3k + 2$. The simplicity of this system of invariants rests upon the fact that $\phi$ and $\psi$ are biquadratics (involving only even powers of the variables). For the outstanding case $p^n = 4l - 1$, in which $\sqrt{-1}$ does not belong to the field $F$, we proceed to show that no biquadratic (whether involving irrationalities or not) is invariant under a $G_{24}$ with coefficients in $F$. Indeed, we show that no biquadratic, other than a perfect square,‡ is invariant under a cyclic transformation $S$ of period 3 with coefficients in $F$. Let the factors be $x \pm cy$, $x \pm dy$. Then, apart from multiplicative constants, $S$ leaves one factor unaltered and permutes the remaining three. Since $S$ is of period 3, it has the form

$$S = \begin{pmatrix} e & f \\ g & -1-e \end{pmatrix},$$

with the characteristic equation $\omega^2 + \omega + 1 = 0$. Since $p \neq 3$, $S$ leaves no

* "Ikosaeder," p. 38.

† *Ibid.*, p. 51.

‡ Such a quartic is not invariant under a $G_{24}$.

linear function absolutely unaltered. Let therefore $S$ multiply $x - cy$ by a cube root $\omega$ of unity. The resulting conditions determine $e$ and $f$. Thus

$$S = \begin{pmatrix} cg + \omega & c\omega^2 - c\omega - c^2 g \\ g & \omega^2 - cg \end{pmatrix}.$$

This replaces $x + cy$ by $x + dy$, where*

$$d(2cg + \omega) = 2c\omega^2 - c\omega - 2c^2 g.$$

Since $S$ shall replace $x + dy$ by $x - dy$, we get

$$-d = -c + \omega^2(c + d)/(cg + dg + \omega).$$

Eliminating $d$, we find that

$$(2cg - \omega^2 + \omega)^2 = -1.$$

Hence the coefficient $cg + \omega$ in $S$ equals $\frac{1}{2}(-1 \pm i)$, which is not in $F$.

Without imposing any restriction on the order $p^n$ of $F$ other than $p > 3$, we determine all sets of generators of $G_{24}$ satisfying relations (11) and such that

$$C = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}. \tag{32}$$

Note that all cyclic $C_3$ are conjugate under $\Gamma$; we choose a simple operator $C$ in order that the quartic invariants shall be simple. Since $A$ shall have period 4,

$$A = \begin{pmatrix} c & d \\ e & -c \end{pmatrix}, \quad B = C^{-1}AC = \begin{pmatrix} d - c & d - 2c - e \\ -d & c - d \end{pmatrix}. \tag{33}$$

The conditions for $C^{-1}BC = AB$ and $|A| = 1$ reduce to

$$e = 1 + d - c, \quad c^2 - cd + d^2 + d + 1 = 0. \tag{34}$$

The points invariant under $C$ are $(\omega, 1)$ and $(\omega^2, 1)$, where $\omega$ is a cube root $\neq 1$ of unity. Under $G_{24}$, $x - \omega y$ and $x + r_i y$ $(i = 1, 2, 3)$ form a conjugate system, where†

$$r_1 = \frac{c - \omega^2}{c - d}, \quad r_2 = \frac{c - d}{\omega^2 - d}, \quad r_3 = \frac{\omega^2 - d}{\omega^2 - c}. \tag{35}$$

Evidently $r_1 r_2 r_3 = -1$. We find that

$$\sigma = r_1 + r_2 + r_3 = (3c^2 d + 2cd + 2c^2 + 2c + d - \omega)/D,$$
$$D = c(c - d)(1 + d) = c + c^2 + c^3,$$
$$\Sigma r_1 r_2 = -\Sigma \frac{1}{r_1} = \sigma - 3.$$

---

* The coefficient of $d$ and denominator in $-d$ are not zero, since $y$ is not a factor of the quartic by hypothesis.

† We may avoid the cases in which a denominator vanishes. Note that $c = 0$ or $d$ requires that $d^2 + d + 1 = 0$ and conversely; that $d = -1$ requires $c^2 + c + 1 = 0$. We treat later the case in which $\omega$ occurs in $F$.

Hence the invariant quartic is

$$Q = (x - \omega y)[x^3 + \sigma x^2 y + (\sigma - 3)xy^2 - y^3]. \tag{36}$$

If we set $g = \sigma - \omega$, we get

$$Q = x^4 + gx^3y + (1 - \omega)(g - 2)x^2y^2 + \omega(4 - g)xy^3 + \omega y^4. \tag{37}$$

If* $p^n = 3k + 1$, $\omega$ belongs to the field. We may then set $c = 0$ and get

$$A = \begin{pmatrix} 0 & \omega \\ -\omega^2 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} \omega & -1 \\ -\omega & -\omega \end{pmatrix}, \tag{38}$$

$$Q = (x^2 - \omega^2 y^2)[x^2 + \tfrac{4}{3}(1 - \omega^2)xy - \omega^2 y^2]. \tag{39}$$

When $Q$ is known, we can by simple differentiation (Klein, *l. c.*, p. 52) determine another quartic and a sextic invariant.

We may also determine $G_{24}$ so that its invariant $G_8$ shall be of the simple form generated by (27). The only transformation $C$ of period 3 and determinant 1 for which $SC = CB$, $BC = CSB$, is

$$C = \begin{pmatrix} \frac{1}{2}(\alpha - \beta - 1) & \frac{1}{2}(\alpha + \beta + 1) \\ \frac{1}{2}(\alpha + \beta - 1) & \frac{1}{2}(-\alpha + \beta - 1) \end{pmatrix}. \tag{40}$$

Now $S$ leaves invariant only $(\pm i, 1)$, $B$ only $(\alpha \pm i, \beta)$, $SB$ only $(\beta \pm i, -\alpha)$, while $B$ interchanges the $(\pm i, 1)$ and also the $(\beta \pm i, -\alpha)$, and $S$ interchanges the $(\alpha \pm i, \beta)$ and also the $(\beta \pm i, -\alpha)$. Further, $C$ replaces $(\pm i, 1)$ by $(\alpha \pm i, \beta)$, the latter by $(\beta \mp i, -\alpha)$, and the last by $(\mp i, 1)$. Hence the six points form a system of conjugates under $G_{24}$. The corresponding invariant is the product of the three quadratic invariants (28) of the $G_8$. The quartic invariants are now more complicated than (37).

In case $p^n = 8h \pm 1$, 2 is a square, and we may extend $G_{24}$ to $G_{48}$ by either of the transformations $D = \begin{pmatrix} a & -a \\ a & a \end{pmatrix}$, $a^2 = 1/2$, which alone have the properties that $D$ is commutative with $S$ and transforms $B$ into $SB$.

---

* In the contrary case we employ suitable products of the invariants derived from (37).